IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

HARDWIRE, LLC,	*	
Plaintiff	*	
v.	*	**CIVIL NO. JKB-20-0304**
IRVIN EBAUGH IV, et al.,	*	
Defendants	*	

* * * * * * * * * * * *

MEMORANDUM

Hardwire, LLC ("Hardwire") filed suit against Irvin Ebaugh IV ("Ebaugh") and Infrastructure Armor, LLC ("IA," and collectively with Ebaugh, the "Defendants"), alleging (i) violation of the Defend Trade Secrets Act, 18 U.S.C. § 1836 *et seq.*; (ii) violation of the Maryland Uniform Trade Secrets Act, Md. Code Ann. Com. Law § 11-1201 *et seq.*; (iii) breach of contract; (iv) violation of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1961 *et seq.*; (v) conversion; (vi) tortious interference with prospective advantage and business relationships; (vii) breach of duty of loyalty and negligence; (viii) unfair competition; and (ix) trespass. Defendants filed a motion to dismiss Hardwire's common law claims for conversion, tortious interference, unfair competition, and trespass (Mot. Dismiss, ECF No. 22), and the matter is fully briefed. No hearing is required. *See* Local Rule 105.6 (D. Md. 2018). For the reasons set forth below, Defendants' motion to dismiss will be denied.

I. Background[1]

Founded in 2000, Hardwire specializes in the development of protective armor for a wide variety of public uses, including "military and law enforcement vehicles, boats, and aircraft, body armor for United States warfighters and law enforcement personnel, and protective materials for public facilities, schools, and courthouses." (Compl. ¶¶ 25, 27, ECF No. 1.) Hardwire maintains more than 20 patents, but most of its proprietary information constitutes "trade secrets that derive independent economic value from not being generally known or readily ascertainable through proper means, rendering the patent process an ineffective means of protection." (*Id.* ¶¶ 32–33.) These trade secrets include "armor recipes and technology, information about test devices and testing methodology, threat information, manufacturing processes, pricing models, and subcontractor information." (*Id.* ¶ 34.)

This case concerns Hardwire's bridge security solutions, which are designed to reinforce bridges against a range of accidents and terrorist attacks. (*Id.* ¶¶ 28–29.) For the past 18 years, Hardwire has invested millions of dollars to develop its bridge armor technology. (*Id.* ¶ 28.) Hardwire's investments have led to the creation of first-in-kind bridge security solutions, and as a result, before the events forming the basis of its Complaint, Hardwire was the frequent recipient of "sole-source contracts . . . without the need for competitive procurement." (*Id.* ¶¶ 30–31.)

In 2002, Ebaugh began working at Hardwire as one of the company's two IT system administrators, a role which gave him "unrestricted access to Hardwire's confidential and proprietary information, trade secrets, and financial data." (*Id.* ¶¶ 42, 50.) Ebaugh advanced at Hardwire, and ultimately, he was promoted to become the Vice President and Program Manager of Hardwire's bridge security division. (*Id.* ¶ 43.) Through this position, "Ebaugh had sufficient

[1] The facts in this section are taken from the Complaint and construed in the light most favorable to the plaintiff. *Ibarra v. United States*, 120 F.3d 472, 474 (4th Cir. 1997).

background, training, and experience to understand the significance and propriety of Hardwire's armor recipes and technology, as well as in-depth knowledge and understanding of Hardwire's test devices and testing methodology, threat information, manufacturing processes, pricing models, and subcontractor information." (*Id.* ¶ 50.)

As a condition of his employment, Ebaugh signed the Company Handbook and Employment Agreement. (*Id.* ¶¶ 44–45.) The Employment Agreement provided:

> All records, files, manuals, any form of electronic media, photo/video graphic materials, software, keys, equipment, credit cards or other tangible material, and all other documents, including but not limited to Confidential Information, relating to the Business of the Company (collectively "Property") that Employee uses, develops, receives, acquires or produces during his employment, are the exclusive Property of the Company. . . . At any time upon demand and upon the termination of his employment, Employee shall return to the Company all Property and all copies of such Property of the Company in his possession or control. Employee shall not make or retain any copies of any Property.

(*Id.* ¶ 49 (quoting Employment Agreement, ¶ 11).)

After working at Hardwire for more than 10 years, Ebaugh's attitude and demeanor around the office became increasingly negative in early 2013. (*Id.* ¶ 10.) Sensing that his working relationship with Hardwire would soon end through either termination or resignation, Ebaugh requested a thumb drive from Hardwire's IT manager on February 22, 2013, and "intentionally and impermissibly downloaded Hardwire's proprietary and confidential data and trade secrets onto the thumb drive" at some point between February 22 and 25, 2013. (*Id.* ¶ 11.) Hardwire terminated Ebaugh on February 25, 2013, after Ebaugh "partially cleaned out his office on Friday, February 22, 2013 and sent inflammatory emails to Hardwire's CEO over the weekend of February 23–24, 2013." (*Id.* ¶ 12.) As soon as Ebaugh was informed of his termination, he went to his office and grabbed the thumb drive with Hardwire's confidential data. (*Id.*) As Ebaugh left the building, "a tussle ensued" when Hardwire executives tried to stop Ebaugh from taking the thumb drive and a

notebook, although Hardwire did not know what was on the thumb drive at the time. (*Id.* ¶ 13.) Ebaugh escaped the skirmish and ran away with the thumb drive, which contained more than "27,000 confidential files." (*Id.* ¶¶ 13, 111.)

Additionally, almost two years after his termination from Hardwire, Ebaugh trespassed on Hardwire's property and either looked over or through the privacy fence to take pictures of "Hardwire's tested bridge armor parts" on or about January 1, 2015. (*Id.* ¶ 17.)

Although Hardwire was not initially aware of Ebaugh's alleged misconduct, Hardwire became suspicious shortly after Ebaugh's termination, when a bridge cable manufacturer that had previously worked with Hardwire stopped responding to Hardwire about proposed collaborations and declined to sign a long-term agreement contemplated by a previous Memorandum of Understanding between the two companies. (*Id.* ¶¶ 62–64.) Upon hearing that Ebaugh had been communicating with Hardwire's suppliers and that IA, Ebaugh's new venture, had won a multi-million-dollar contract to provide armor protection for the Kosciuszko Bridge, Hardwire contacted the FBI to report a possible theft and misappropriation of "sensitive materials" in early 2015. (*Id.* ¶¶ 72–74.)

In February 2016, Hardwire entered into an agreement with Defendants to toll the statute of limitations with respect to Hardwire's claims without interfering with ongoing investigations of the FBI and other governmental agencies. (*Id.* ¶ 100.) Hardwire brought this lawsuit on February 4, 2020, alleging violations of federal and state law as well as state common law claims. (ECF No. 1.) Defendants filed a motion to dismiss Hardwire's common law claims for conversion, tortious interference, unfair competition, and trespass on the grounds that those claims are

preempted by the displacement provision in the Maryland Uniform Trade Secrets Act ("MUTSA"), Md. Code Ann. Com. Law ("CL") § 11-1207. (Mot. Dismiss at 1–2.)

II. Legal Standard

To survive a motion to dismiss, "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). Facial plausibility exists "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* at 678. An inference of a mere possibility of misconduct is insufficient to support a plausible claim. *Id.* at 679. Rather, "[f]actual allegations must be enough to raise a right to relief above the speculative level." *Twombly*, 550 U.S. at 555. "A pleading that offers 'labels and conclusions' or . . . 'naked assertion[s]' devoid of 'further factual enhancement'" will not suffice. *Iqbal*, 556 U.S. at 678 (alteration in original) (quoting *Twombly*, 550 U.S. at 555, 557). Although when considering a motion to dismiss, a court must accept as true all factual allegations in the complaint, this principle does not apply to legal conclusions couched as factual allegations. *Twombly*, 550 U.S. at 555.

III. Analysis

Derived from the Uniform Trade Secrets Act ("UTSA"), MUTSA creates a cause of action for the misappropriation of trade secrets. A trade secret is defined as information which (1) generates "independent economic value" from not being widely known; and (2) "[i]s the subject of efforts that are reasonable under the circumstances to maintain its secrecy." CL § 11-1201(e). Misappropriation occurs through (1) acquisition of a trade secret by improper means; or (2) disclosure or use of a trade secret without express or implied consent. CL § 11-1201(c); *see also Trandes Corp. v. Guy F. Atkinson Co.*, 996 F.2d 655, 660 (4th Cir. 1993) ("To prove

misappropriation of a trade secret . . . a plaintiff must show (1) that it possessed a valid trade secret, (2) that the defendant acquired its trade secret, and (3) that the defendant knew or should have known that the trade secret was acquired by improper means").

MUTSA provides the sole civil remedy for misappropriation of a trade secret and as such "displaces conflicting tort, restitutionary, and other law of this State providing civil remedies" for such conduct. CL § 11-1207(a); *see LeJeune v. Coin Acceptors, Inc.*, 849 A.2d 451, 461 (Md. 2004). MUTSA's displacement provision carves out three exceptions for actions that are not preempted by the statute, including "[o]ther civil remedies that are not based upon misappropriation of a trade secret." CL § 11-1207(b)(1)(ii).

Defendants have moved to dismiss Hardwire's common law claims for conversion (Count V), tortious interference with prospective advantage and business relationships (Count VI), unfair competition (Count VIII), and trespass (Count IX) on the grounds that all four of these claims "are grounded in the same operative facts as its MUTSA Count and, as such, are preempted."[2] (Mot. Dismiss Mem. Supp. at 6, ECF No. 22-1.) The Court considers whether each Count is preempted by MUTSA in turn and concludes that all four common law claims survive Defendants' motion to dismiss.

A. Preemption of Other Civil Remedies Under MUTSA

The Maryland Court of Appeals has not addressed the scope of MUTSA preemption,[3] and divergent interpretations of the UTSA's displacement provision have emerged in jurisdictions

---

[2] In their motion to dismiss, Defendants do not address the elements of each common law claim. Accordingly, the Court will assume without deciding that Hardwire has alleged the necessary elements of each distinct claim for the purposes of the pending motion and refrain from testing arguments not raised by Defendants.

[3] The Maryland Court of Special Appeals has referenced the scope of MUTSA preemption twice in *dicta*. *See Bond v. Polycycle, Inc.*, 732 A.2d 970, 976 n.2 (Md. Ct. Spec. App. 1999) (explaining that a common law claim, "if based solely on misappropriation of a trade secret, cannot survive once a remedy under the MUTSA is obtained"); *see also First Union Nat'l Bank v. Steele Software Sys. Corp.*, 838 A.2d 404, 434 n.16 (Md. Ct. Spec. App. 2003) (finding

around the country. *See Allstate Ins. Co. v. Warns*, Civ. No. CCB-11-1846, 2012 WL 681792, at *8 (D. Md. Feb. 29, 2012). Some courts have given the provision broad effect, finding that "the UTSA preempts all common law tort claims based on misappropriation of information, whether or not it meets the statutory definition of a trade secret." *See, e.g.*, *Firetrace USA, LLC v. Jesclard*, 800 F. Supp. 2d 1042, 1048 (D. Ariz. 2010) (citing *Hauck Mfg. v. Astec Industries, Inc.*, 375 F. Supp. 2d 649, 654 (E.D. Tenn. 2004)). Others, including courts in the District of Maryland, have found that the UTSA (and specifically, MUTSA) preempts only claims based on misappropriation of trade secrets, not other confidential information. *See, e.g.*, *Equity Prime Mortg., LLC v. 1st Fin., Inc.*, Civ. No. GLR-17-3754, 2019 WL 859135, at *8 (D. Md. Feb. 22, 2019); *Structural Pres. Sys. LLC v. Andrews*, Civ. No. MJG-12-1850, 2013 WL 3820023, at *5 (D. Md. July 23, 2013); *Swedish Civil Aviation Admin. v. Project Mgmt. Enters., Inc.*, 190 F. Supp. 2d 785, 802 (D. Md. 2002).

Courts in this District have held that plaintiffs may plead in the alternative under the liberal federal pleading standards that misappropriated confidential information is not a trade secret, and as such, common law claims relating to such confidential information are not preempted by MUTSA. *Telogis, Inc. v. InSight Mobile Data, Inc.*, Civ. No. PWG-14-563, 2014 WL 7336678, at *5 (D. Md. Dec. 19, 2014); *Swedish Civil Aviation*, 190 F. Supp. 2d at 802. Federal Rule of Civil Procedure 8(e)(2) provides, "[a] party may . . . state as many separate claims or defenses as the party has regardless of consistency and whether based on legal [or] equitable . . . grounds." Fed. R. Civ. P. 8(e)(2). As such, "[p]arties may plead alternative theories of liability, indeed as many theories as the facts will fit." *Polar Communications Corp. v. Oncor Communications, Inc.*, 927 F. Supp. 894, 896 (D. Md. 1996). In *Telogis*, for instance, the court found that the plaintiff's

---

that the plaintiff's common law fraud claim would have been preempted by MUTSA had the plaintiff not "*repeatedly renounced* any claim that First Union stole or misappropriated trade secrets") (emphasis in original).

unfair competition claim was not preempted by MUTSA where the plaintiff alleged that the defendants unfairly obtained and used both trade secrets and "Confidential Business Information." 2014 WL 7336678, at *5. Although acknowledging that "any and all of [the Confidential Business Information] could qualify as trade secrets," the court held that the claim was permitted as a pleading in the alternative until the court made such a determination. *Id.*

1. Count V: Conversion

Defendants rely on *Omni Direct, Inc. v. Creative Direct Response, Inc.*, 2018 Md. Cir. Ct. LEXIS 12 (Md. Cir. Ct. Dec. 18, 2018), a recent case in the Circuit Court of Maryland for Montgomery County, to argue that Hardwire's conversion claim is preempted because it is "founded upon the same facts that support its MUTSA claim." (Mot. Dismiss Mem. Supp. at 8.) In *Omni Direct*, the court found that the plaintiff's common law claims were preempted where they were "grounded in the same facts" supporting the MUTSA claim and there were "no theories of relief that are supported by facts unrelated to the misappropriation of trade secrets claim." 2018 Md. Cir. Ct. LEXIS 12, at *13. The court rejected the "stringent approach" limiting the scope of the displacement provision to trade secrets, arguing that "this approach leads to exactly what was sought to be avoided by the Uniform Act: pleading in the alternative that something both is and is not a trade secret in the same complaint, and then adding nearly every conceivable common law count to the same set of operative facts which also constitutes the misappropriation of trade secrets." *Id.* at *7–8. The court explained that although the Maryland Rules of Civil Procedure allow pleading in the alternative, "that is not a cogent reason to disregard an express statutory displacement provision." *Id.* at *10 n.30.

The Court disagrees with this expansive interpretation of the scope of MUTSA preemption, and at any rate, Hardwire's Complaint is distinguishable from the pleadings in *Omni Direct*. As

explained above, MUTSA's displacement provision states that it does not preempt "[o]ther civil remedies that are not based upon misappropriation of a *trade secret*." CL § 11-1207(b)(1)(ii) (emphasis added). The *Omni Direct* court's broad interpretation of MUTSA's displacement provision could result in the preemption of claims not based upon the misappropriation of trade secrets in contravention of the statute's plain meaning if a court ultimately concluded that confidential information at issue did not constitute a trade secret. As such, prohibiting pleadings in the alternative could deprive a claimant of a meritorious cause of action. Additionally, this case also distinguishes the pleadings in *Omni Direct*. While the plaintiff in *Omni Direct* pled that all of its misappropriated information constituted trade secrets, 2018 Md. Cir. Ct. LEXIS 12, at *11, Hardwire alleged that Ebaugh stole both "confidential information and trade secrets." (Compl. ¶ 63.)

The Court agrees with Hardwire that the conversion claim is a permissible pleading in the alternative under the Federal Rules of Civil Procedure. Hardwire claims that "Ebaugh stole a thumb drive and notebook, owned by Hardwire, containing over 27,000 of Hardwire's files consisting of Hardwire's *confidential information and trade secrets*." (Compl. ¶ 163) (emphasis added.) To the extent that any files on the allegedly stolen thumb drive constituted trade secrets, Hardwire's conversion claim is based on the misappropriation of trade secrets and is preempted as such under MUTSA. *See* CL § 11-1207; *Bond v. Polycycle, Inc.*, 732 A.2d 970, 976 n.2 (Md. Ct. Spec. App. 1999) (explaining that a common law claim, "if based *solely on misappropriation of a trade secret*, cannot survive once a remedy under the MUTSA is obtained") (emphasis added). Hardwire does not plead, however, that all of the allegedly stolen information constituted trade secrets. The determination of what constitutes a trade secret "is a conclusion of law based upon the applicable facts." *Telogis*, 2014 WL 7336678, at *5 (quoting *Structural Pres. Sys.*, 2013 WL

3820023, at *5). Although, as in *Telogis*, it is possible that the Court will ultimately conclude that the alleged confidential information at issue does constitute trade secrets, the conversion claim will be permitted as a pleading in the alternative at least until the Court makes this finding. *Id.* at *5; *see also Equity Prime Mortg.*, 2019 WL 859135, at *8 (declining to dismiss the plaintiff's conversion claim as preempted by MUTSA before the plaintiff further specified which information constituted trade secrets).

2. *Count VI: Tortious Interference with Prospective Advantage and Business Relationships*

Defendants likewise rely on *Omni Direct* to support the argument that Hardwire's tortious interference claim is preempted because it uses "the same improper acquisition and use fact allegations used to support its MUTSA claim." (Mot. Dismiss. Mem. Supp. at 4.)

Defendants' argument is unavailing because as Hardwire points out, Hardwire's tortious interference claim is not based entirely on the same allegations as its misappropriation of trade secrets claim. (Opp'n to Mot. Dismiss at 8–10, ECF No. 25.) Hardwire alleges that Defendants tortiously interfered with Hardwire's business by "misus[ing] Hardwire's confidential pricing information to obtain a competitive advantage against Hardwire in the bidding process" and ultimately depriving Hardwire of the "multi-million-dollar economic opportunity" to provide bridge armor for projects and also of "the opportunity to be awarded the large sole source contract for another large suspender rope project." (Compl. ¶¶ 175–79.) Under Maryland law, a tortious interference claim requires proof of "(1) an intentional and willful act; (2) calculated to cause damage to the plaintiff in his lawful business; (3) done with the unlawful purpose to cause such damage and loss; without right or justifiable cause on the part of the defendants (which constitutes malice); and (4) that caused actual damage or loss." *Paccar Inc. v. Elliot Wilson Capitol Trucks LLC*, 905 F. Supp. 2d 675, 695 (D. Md. 2012). Although Hardwire claims that Defendants' alleged

misappropriation of trade secrets enabled Defendants' alleged tortious interference, this common law claim is based on the fact of the interference, not "the specific fruits of the interference." *See Equity Prime Mortg.*, 2019 WL 859135, at *7. In other words, Hardwire could succeed in its tortious interference claim without a showing that Defendants misappropriated its trade secrets. *See Smithfield Ham & Prods. Co. v. Portion Pac*, 905 F. Supp. 346, 350 (E.D. Va. 1995) ("[t]he question is not whether success on the misappropriation claim would provide the relief sought by the common law counts, but whether failure of the misappropriation claim would doom the remaining counts as well"). As such, Hardwire's tortious interference claim is not based on its misappropriation of trade secrets claim, and as a result, is not preempted by MUTSA. *See* CL § 11-1207(b)(ii).

3. Count VIII: Unfair Competition

Defendants argue that Hardwire's unfair competition claim is preempted under *Omni Direct* because "Hardwire alleges the same factual allegations from its MUTSA count to support its unfair competition Count." (Mot. Dismiss. Mem. Supp. at 4.)

As explained above with respect to Hardwire's conversion claim, *supra* § III.A.1, Hardwire's unfair competition claim is a permissible pleading in the alternative. To support its unfair competition claim, Hardwire alleged that "Ebaugh, through IA, wrongfully used and disclosed, and continues to wrongfully use and disclose, Hardwire's *confidential information and trade secrets*" and "thus damaged or jeopardized Hardwire's business through fraud, deceit, trickery, and unfair methods." (Compl. ¶¶ 198–99) (emphasis added.) Although this claim is preempted to the extent it is based on the alleged wrongful use and disclosure—constituting misappropriation—of trade secrets, the unfair competition claim survives at least until the Court

determines what information, if any, qualifies as trade secrets under MUTSA. *See Equity Prime Mortg.*, 2019 WL 859135, at *8.

4. Count IX: Trespass

Defendants also rely on *Omni Direct* to support the contention that Hardwire's trespass claim is displaced because it was "founded upon the same facts that support its MUTSA claim." (Mot. Dismiss. Mem. Supp. at 8.)

In response, Hardwire argues that its trespass claim is not based on the misappropriation of trade secrets because the claim "is not reliant on Hardwire establishing a theft of its trade secrets." (Opp'n to Mot. Dismiss at 11.) Further, Hardwire maintains, a trespass claim concerns a wrongful interference with property, and as such, "[t]he acts taking place *after* the interference occurred may be separately actionable, but they are not duplicative of the trespass claim." (*Id.*) (emphasis in original.)

Although this claim constitutes a permissible alternative pleading at this stage, Hardwire's trespass claim is preempted to the extent that Hardwire alleges Ebaugh improperly acquired trade secrets by trespassing. Hardwire claims that "Ebaugh physically and unlawfully entered upon Hardwire's private property" and "gained an elevated potion [*sic*] so that he could see over or through Hardwire's privacy fence." (Compl. ¶¶ 204–05.) From that vantage point, Ebaugh "took photographs of Hardwire's tested bridge armor parts, zooming in on specific design features." (*Id.* ¶ 205.) In the event that all of the alleged confidential information contained in these alleged images constitute trade secrets, a claim that Ebaugh trespassed on Hardwire's private property to take pictures of the tested bridge armor parts would amount to an allegation that he used improper means to acquire Hardwire's trade secrets under MUTSA. *See* CL § 11-1201(c)(1) (defining misappropriation as the "[a]cquisition of a trade secret of another by a person who knows or has

reason to know that the trade secret was acquired by improper means"); *Id.* at § 11-1201(b) (explaining that "'[i]mproper means' includes . . . espionage through electronic or other means"). As a result, to the extent Ebaugh's alleged photographs of the bridge armor parts captured trade secret information, Hardwire's trespass claim is preempted. *See Equity Prime Mortg.*, 2019 WL 859135, at *8–9 (explaining that MUTSA preempts common law claims to the extent that they are based on misappropriation of trade secrets). Although it seems likely that, if they are confidential, Hardwire's "specific design features" would constitute trade secrets, the Court refrains from making this conclusion of law at this juncture, and Hardwire's trespass claim survives as a pleading in the alternative to the extent that it concerns confidential information that does not rise to the level of a trade secret under MUTSA. *See id.* at *8 (declining to dismiss the plaintiff's conversion claim "[a]t this pre-discovery stage, before Equity further specifies which items of information are trade secrets"); *supra* §§ III.A.1, 3.

IV. Conclusion

For the foregoing reasons, an Order shall enter denying Defendants' motion to dismiss Hardwire's conversion (Count V), tortious interference (Count VI), unfair competition (Count VIII), and trespass (Count IX) claims.

DATED this 26 day of August, 2020.

BY THE COURT:

James K. Bredar

James K. Bredar
Chief Judge